

CLAIMS

1 1. In a prime number generating system including a processing unit and a plurality
2 of exponentiation units communicatively coupled with the processing unit, a process of
3 searching in parallel for a plurality of prime number values substantially simultaneously,
4 comprising the steps of:
5 randomly generating a plurality of k random odd numbers each providing a prime
6 number candidate; and
7 performing at least one primality test on each of said candidates, each of said primality
8 tests including an associated exponentiation operation executed by an associated one of the
9 exponentiation units, said exponentiation operations being performed by said associated
10 exponentiation units substantially simultaneously.

1 2. In a prime number generating system as recited in claim 1 wherein said plurality of k
2 randomly generated numbers are expressed as $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$, further comprising the steps
3 of:
4 determining a plurality of y additional odd numbers based on each one of the randomly
5 generated numbers $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$ to provide $(k \times y)$ additional prime number candidates $(n_{0,1}$
6 $, n_{0,2}, \dots n_{0,y}), (n_{1,1}, n_{1,2}, \dots n_{1,y}), \dots (n_{(k-1),1}, n_{(k-1),2}, \dots n_{(k-1),y})$ thereby yielding a total number of $(k$
7 $\times (y+1))$ prime number candidates;
8 wherein said step of performing includes performing a primality test on each of said total
9 number $(k \times (y+1))$ of candidates, each of the plurality of $(k \times (y+1))$ primality tests including an
10 associated exponentiation operation executed by an associated one of a plurality of $(k \times (y+1))$ of
11 the exponentiation units, said exponentiation operations being performed by said plurality of $(k \times$
12 $(y+1))$ exponentiation units substantially simultaneously.

1 3. In a prime number generating system as recited in claim 2 wherein each of said plurality
2 of prime number values being searched for has a specified length, and wherein said plurality of y
3 additional odd numbers defines an interval that is selected relative to said specified length.

1 4. In a prime number generating system as recited in claim 2 wherein said step of
2 determining a plurality of y additional odd numbers based on each one of the randomly
3 generated numbers $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$ includes successively adding two to each of said randomly
4 generated odd numbers $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$ to provide $(k \times y)$ additional prime number candidates
5 expressed as $(n_{0,1} = n_{0,0} + 2, n_{0,2} = n_{0,0} + 4, \dots n_{0,y} = n_{0,0} + (y \cdot 2)), (n_{1,1} = n_{1,0} + 2, n_{1,2} = n_{1,0} + 4, \dots$
6 $n_{1,y} = n_{1,0} + (y \cdot 2)), \dots (n_{(k-1),1} = n_{(k-1),0} + 2, n_{(k-1),2} = n_{(k-1),0} + 4, \dots n_{(k-1),y} = n_{(k-1),0} + (y \cdot 2))$.

1 5. In a prime number generating system as recited in claim 1 wherein said step of
2 performing includes performing a plurality of t primality tests on each one of said plurality of k
3 randomly generated numbers, each of the plurality of $(k \times t)$ primality tests including an
4 associated exponentiation operation executed by an associated one of a plurality of $(k \times t)$ of the
5 exponentiation units, said exponentiation operations being performed by said associated
6 exponentiation units substantially simultaneously.

1 6. In a prime number generating system as recited in claim 2 wherein said step of
2 performing includes performing a plurality of t primality tests on each of said $(k \times (y+1))$ prime
3 number candidates, each of the plurality of $(k \times (y+1) \times t)$ primality tests including an associated
4 exponentiation operation executed by an associated one of a plurality of $(k \times (y+1) \times t)$ of the
5 exponentiation units, said exponentiation operations being performed by said plurality of $(k \times$
6 $(y+1) \times t)$ exponentiation units substantially simultaneously.

1 7. In a prime number generating system as recited in claim 1 further comprising the steps
2 of:

3 sieving said prime number candidates by performing a small divisor test on each
4 of said candidates in order to eliminate candidates revealed to be composite numbers by
5 said small divisor test thereby yielding a sieved number s of candidates;

6 wherein said step of performing includes performing at least one primality test on each of
7 said sieved number s of candidates, each of the plurality of s primality tests including an
8 associated exponentiation operation executed by an associated one of a plurality of s of the
9 exponentiation units, said exponentiation operations being performed by said plurality of s
10 exponentiation units substantially simultaneously.

1 8. In a prime number generating system as recited in claim 7 further comprising the steps
2 of:
3 receiving a specified public exponent e associated with a cryptographic application;
4 testing the suitability of each of said prime number candidates for use in said
5 cryptographic application by testing the relative primality of each said prime number candidate
6 minus one and said specified public exponent e , wherein said step of testing the suitability is
7 performed prior to said step of performing at least one primality test.

1 9. In a prime number generating system as recited in claim 2 further comprising the steps
2 of:
3 sieving said prime number candidates by performing a small divisor test on each
4 of said number $(k \times (y+1))$ of prime number candidates in order to eliminate candidates
5 revealed to be composite numbers by said small divisor test thereby yielding a sieved
6 number s of candidates;
7 wherein said step of performing includes performing at least one primality test on
8 each of said sieved number s of candidates, each of the plurality of s primality tests
9 including an associated exponentiation operation executed by an associated one of a
10 plurality of s of the exponentiation units, said exponentiation operations being performed
11 by said plurality of s exponentiation units substantially simultaneously.

1 10. In a prime number generating system as recited in claim 1 further comprising the step of:
2 sieving said prime number candidates by performing a small divisor test on each
3 of said candidates in order to eliminate candidates revealed to be composite numbers by
4 said small divisor test thereby yielding a sieved number s of candidates;
5 wherein said step of performing includes performing an associated first one of t primality
6 test on each of said sieved number s of candidates, each of the plurality of s first primality tests
7 including an associated exponentiation operation executed by an associated one of a plurality of s
8 of the exponentiation units, said first exponentiation operations being performed by said plurality
9 of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to
10 be composite numbers by said first primality tests thereby yielding a remaining number r of
11 candidates; and

performing a plurality of $t-1$ additional primality tests on each of said remaining number r of candidates, each of the plurality of $(r \times (t-1))$ primality tests including an associated exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the exponentiation units, said $(r \times (t-1))$ exponentiation operations being performed by said plurality of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further candidates revealed to be composite numbers.

11. In a prime number generating system as recited in claim 2 further comprising the step of: sieving said prime number candidates by performing a small divisor test on each of said number $(k \times (y+1))$ of prime number candidates in order to eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number s of candidates;

wherein said step of performing includes performing an associated first one of t primality tests on each of said sieved number s of candidates, each of the plurality of s first primality tests including an associated exponentiation operation executed by an associated one of a plurality of s of the exponentiation units, said first exponentiation operations being performed by said plurality of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to be composite numbers by said first primality tests thereby yielding a remaining number r of candidates; and

performing a plurality of $t-1$ additional primality tests on each of said remaining number r of candidates, each of the plurality of $(r \times (t-1))$ primality tests including an associated exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the exponentiation units, said $(r \times (t-1))$ exponentiation operations being performed by said plurality of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further candidates revealed to be composite numbers.

12. In a prime number generating system as recited in claim 1 wherein said step of performing at least one primality test includes performing a Fermat type primality test.

13. In a prime number generating system as recited in claim 1 wherein said step of performing at least one primality test includes performing a Miller-Rabin type primality test.

1 14. In a prime number generating system as recited in claim 1 wherein said step of randomly
2 generating a plurality of k random odd numbers further includes:

3 defining a length L for each of the plurality of k random numbers to be generated;
4 and

5 generating each of said plurality of k random odd numbers in an interval between
6 2^L and 2^{L-1} .

1 15. In a prime number generating system including a processing unit and a plurality
2 of exponentiation units communicatively coupled with the processing unit, a process of
3 searching in parallel for a plurality of prime number values simultaneously, comprising
4 the steps of:

5 randomly generating at least one random odd number providing a prime number
6 candidate;

7 determining a plurality of y additional odd numbers based on said at least one randomly
8 generated odd number to provide y additional prime number candidates, thereby providing a total
9 number of y+1 candidates;

10 performing at least one primality test on each of said y+1 candidates, each of the y+1
11 primality tests including an associated exponentiation operation executed by an associated one of
12 y+1 of the exponentiation units, said y+1 exponentiation operations being performed by said
13 associated y+1 exponentiation units substantially simultaneously.

1 16. In a prime number generating system as recited in claim 15 wherein said at least one
2 randomly generated odd number is expressed as $n_{0,0}$, and wherein said step of determining a
3 plurality of y additional odd numbers based on said randomly generated odd number $n_{0,0}$ includes
4 successively adding two to said randomly generated odd number $n_{0,0}$ to provide (y+1) additional
5 prime number candidates expressed as ($n_{0,1} = n_{0,0} + 2$, $n_{0,2} = n_{0,0} + 4$, ... $n_{0,y} = n_{0,0} + (y \cdot 2)$).

1 17. In a prime number generating system as recited in claim 15 wherein said step of
2 performing includes performing a plurality of t primality tests on each of said (y+1) prime
3 number candidates, each of the plurality of ((y+1) x t) primality tests including an associated
4 exponentiation operation executed by an associated one of a plurality of ((y+1) x t) of the

5 exponentiation units, said exponentiation operations being performed by said plurality of $((y+1) \times$
6 $t)$ exponentiation units substantially simultaneously.

1 18. In a prime number generating system as recited in claim 15 further comprising the step of
2 sieving said $y+1$ candidates by performing a small divisor test on each of said candidates in order
3 to eliminate candidates revealed to be composite numbers by said small divisor test thereby
4 yielding a sieved number s of candidates.

1 19. In a prime number generating system as recited in claim 18 further comprising the
2 step of:
3 receiving a specified public exponent e associated with a cryptographic application;
4 testing the suitability of each of said prime number candidates for use in said
5 cryptographic application by testing the relative primality of each said prime number candidate
6 minus one and said specified public exponent e , wherein said step of testing the suitability is
7 performed prior to said step of performing at least one primality test.

1 20. In a prime number generating system as recited in claim 15 further comprising the
2 step of:
3 sieving said $y+1$ candidates by performing a small divisor test on each of said
4 candidates in order to eliminate candidates revealed to be composite numbers by said
5 small divisor test thereby yielding a sieved number s of candidates;
6 wherein said step of performing includes performing an associated first one of t primality
7 test on each of said sieved number s of candidates, each of the plurality of s first primality tests
8 including an associated exponentiation operation executed by an associated one of a plurality of s
9 of the exponentiation units, said first exponentiation operations being performed by said plurality
10 of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to
11 be composite numbers by said first primality tests thereby yielding a remaining number r of
12 candidates; and
13 performing a plurality of $t-1$ additional primality tests on each of said remaining number
14 r of candidates, each of the plurality of $(r \times (t-1))$ first primality tests including an associated
15 exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the

16 exponentiation units, the $(r \times (t-1))$ exponentiation operations being performed by said plurality
17 of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further
18 candidates revealed to be composite numbers.

1 21. In a prime number generating system as recited in claim 15 wherein said step of
2 performing at least one primality test includes performing a Fermat type primality test.

1 22. In a prime number generating system as recited in claim 15 wherein said step of
2 performing at least one primality test includes performing a Miller-Rabin type primality test.

1 23. In a prime number generating system as recited in claim 15 wherein said step of
2 randomly generating at least one random odd number further includes:
3 defining a length L for each of the plurality of k random numbers to be generated;
4 and
5 generating each of said plurality of k random odd numbers in an interval between 2^L and
6 2^{L-1} .

1 24. In a prime number generating system including a processing unit and a plurality
2 of exponentiation units communicatively coupled with the processing unit, a process of
3 searching in parallel for a plurality of prime number values simultaneously, comprising
4 the steps of:
5 randomly generating at least one random odd number providing a prime number
6 candidate; and
7 testing the primality of said candidate by performing a plurality of t primality tests on
8 said candidate, each of the plurality of the t primality tests including an associated exponentiation
9 operation executed by an associated one of a plurality of t of the exponentiation units, said
10 exponentiation operations being performed by said plurality of t exponentiation units
11 substantially simultaneously.

1 25. In a prime number generating system as recited in claim 24 further including the step of
2 sieving said candidates by performing a small divisor test on each of said candidates in order to

eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number s of candidates.

26. In a prime number generating system as recited in claim 25 further including the step of:
receiving a specified public exponent e associated with a cryptographic application;
testing the suitability of each of said prime number candidates for use in said cryptographic application by testing the relative primality of each said prime number candidate minus one and said specified public exponent e , wherein said step of testing the suitability is performed prior to said step of performing at least one primality test.

27. In a prime number generating system as recited in claim 24 wherein said step of testing the primality of said candidate further includes:

sieving said candidates by performing a small divisor test on each of said candidates in order to eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number s of candidates;

performing an associated first one of said t primality test on each of said sieved number s of candidates, each of the plurality of s first primality tests including an associated exponentiation operation executed by an associated one of a plurality of s of the exponentiation units, said first exponentiation operations being performed by said plurality of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to be composite numbers by said first primality tests thereby yielding a remaining number r of candidates; and

performing a plurality of $t-1$ additional ones of said t primality tests on each of said remaining number r of candidates, each of the plurality of $(r \times (t-1))$ first primality tests including an associated exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the exponentiation units, said $(r \times (t-1))$ exponentiation operations being performed by said plurality of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further candidates revealed to be composite numbers.

28. In a prime number generating system including a processing unit and a plurality of exponentiation units communicatively coupled with the processing unit, a process of

3 searching in parallel for a plurality of prime number values simultaneously, comprising
4 the steps of:
5 randomly generating a plurality of k random odd numbers expressed as $n_{0,0}$, $n_{1,0}$,
6 $\dots n_{(k-1),0}$, each said number providing a prime number candidate;
7 determining a plurality of y additional odd numbers based on each one of the randomly
8 generated odd numbers $n_{0,0}$, $n_{1,0}$, $\dots n_{(k-1),0}$ to provide $(k \times y)$ additional prime number candidates
9 $(n_{0,1}, n_{0,2}, \dots n_{0,y})$, $(n_{1,1}, n_{1,2}, \dots n_{1,y})$, $\dots (n_{(k-1),1}, n_{(k-1),2}, \dots n_{(k-1),y})$ thereby yielding a total number
10 of $(k \times (y+1))$ prime number candidates;
11 sieving said $(k \times (y+1))$ prime number candidates by performing a small divisor
12 test on each of said candidates in order to eliminate candidates revealed to be composite
13 numbers by said small divisor test thereby yielding a sieved number s of candidates; and
14 performing at least one primality test on each of said sieved number s of candidates, each
15 of the plurality of s primality tests including an associated exponentiation operation executed by
16 an associated one of a plurality of s of the exponentiation units, said exponentiation operations
17 being performed by said plurality of s exponentiation units substantially simultaneously in order
18 to eliminate candidates revealed to be composite numbers by said primality test thereby yielding
19 a remaining number r of candidates.

1 29. In a prime number generating system as recited in claim 28 wherein said step of
2 determining a plurality of y additional odd numbers based on each one of the randomly
3 generated odd numbers $n_{0,0}$, $n_{1,0}$, $\dots n_{(k-1),0}$ includes successively adding two to each of said
4 randomly generated odd numbers $n_{0,0}$, $n_{1,0}$, $\dots n_{(k-1),0}$ to provide $(k \times y)$ additional prime number
5 candidates expressed as $(n_{0,1} = n_{0,0} + 2, n_{0,2} = n_{0,0} + 4, \dots n_{0,y} = n_{0,0} + (y \cdot 2))$, $(n_{1,1} = n_{1,0} + 2, n_{1,2} =$
6 $n_{1,0} + 4, \dots n_{1,y} = n_{1,0} + (y \cdot 2))$, $\dots (n_{(k-1),1} = n_{(k-1),0} + 2, n_{(k-1),2} = n_{(k-1),0} + 4, \dots n_{(k-1),y} = n_{(k-1),0} +$
7 $(y \cdot 2))$.

1 30. In a prime number generating system as recited in claim 28 further comprising the steps
2 of:
3 performing a plurality of $t-1$ additional primality tests on each of said remaining number
4 r of candidates, each of the plurality of $(r \times (t-1))$ primality tests including an associated
5 exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the

6 exponentiation units, said $(r \times (t-1))$ exponentiation operations being performed by said plurality
7 of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further
8 candidates revealed to be composite numbers.

1 31. In a prime number generating system as recited in claim 28 wherein said step of
2 performing at least one primality test includes performing a Fermat type primality test.

1 32. In a prime number generating system as recited in claim 28 wherein said step of
2 performing at least one primality test includes performing a Miller-Rabin type primality test.

1 33. In a prime number generating system as recited in claim 28 wherein said step of
2 randomly generating a plurality of k random odd numbers further includes:
3 defining a length L for each of the plurality of k random numbers to be generated;
4 and
5 generating each of said plurality of k random odd numbers in an interval between
6 2^L and 2^{L-1} .

1 34. In a prime number generating system as recited in claim 28 wherein k is greater
2 than or equal to 2.

1 35. In a prime number generating system as recited in claim 28 further comprising the
2 steps of:
3 receiving a specified public exponent e associated with a cryptographic application;
4 testing the suitability of each of said prime number candidates for use in said
5 cryptographic application by testing the relative primality of each said prime number
6 candidate minus one and said specified public exponent e, wherein said step of testing the
7 suitability is performed prior to said step of performing at least one primality test.

1 36. A prime number generating system for searching in parallel for a plurality of
2 prime number values simultaneously, comprising:

processing means operative to randomly generate a plurality of k random odd numbers each providing a prime number candidate, and to provide at least one set of test parameters associated with a primality test to be performed on each one of said plurality of k randomly generated numbers, each said set of said test parameters including said associated randomly generated number and an associated base value; and

a plurality of exponentiation units each being communicatively coupled with said processing means, and being responsive to an associated one of said sets of test parameters, and operative to perform an exponentiation operation based on said associated set of test parameters, and also operative to generate a primality test result signal declaring said associated prime number candidate to be either composite or prime with reference to said associated base value, said exponentiation units being operative to perform said exponentiation operations substantially simultaneously;

said processing means being responsive to said primality test result signals, and operative to process said test result signals for the purpose of eliminating randomly generated numbers declared to be composite in accordance with a search for prime number values.

37. A prime number generating system as recited in claim 36 wherein:

said processing means is operative to provide a plurality of t sets of test parameters associated with a plurality of t primality tests to be performed on each one of said plurality of k randomly generated numbers, each of the $(k \times t)$ sets of said test parameters including an associated one of said plurality of k randomly generated numbers and an associated one of a plurality of t base values;

said plurality of exponentiation units includes a plurality of at least $(k \times t)$ exponentiation units each being responsive to an associated one of said $(k \times t)$ sets of said test parameters, and being operative to perform an exponentiation operation based on said associated set of test parameters, and also operative to generate a primality test result signal declaring said associated prime number candidate to be either composite or prime with reference to said associated base value, said plurality of at least $(k \times t)$ exponentiation units being operative to perform said plurality of $(k \times t)$ exponentiation operations substantially simultaneously.

1 38. A prime number generating system as recited in claim 36 wherein said processing
2 means is further operative to sieve said prime number candidates by performing a small
3 divisor test on each of said prime number candidates in order to eliminate candidates
4 revealed to be composite numbers by said small divisor test thereby yielding a sieved
5 number s of candidates.

1 39. A prime number generating system as recited in claim 36 wherein said plurality of k
2 randomly generated odd numbers are expressed as $n_{0,0}, n_{1,0}, \dots, n_{(k-1),0}$, and wherein:
3 said processing means is further operative to develop a plurality of y additional odd
4 numbers based on each one of the randomly generated odd numbers $n_{0,0}, n_{1,0}, \dots, n_{(k-1),0}$ to provide
5 $(k \times y)$ additional prime number candidates $(n_{0,1}, n_{0,2}, \dots, n_{0,y}), (n_{1,1}, n_{1,2}, \dots, n_{1,y}), \dots, (n_{(k-1),1}, n_{(k-1),2},$
6 $\dots, n_{(k-1),y})$ thereby yielding a total number of $(k \times (y+1))$ prime number candidates;
7 said plurality of exponentiation units includes a plurality of at least $(k \times (y+1))$
8 exponentiation units each being responsive to an associated one of said $(k \times (y+1))$ sets of
9 said test parameters, and being operative to perform an exponentiation operation based on
10 said associated set of test parameters, and also operative to generate a primality test result
11 signal declaring said associated prime number candidate to be either composite or prime
12 with reference to said associated base value, said plurality of at least $(k \times (y+1))$
13 exponentiation units being operative to perform the plurality of $(k \times (y+1))$ exponentiation
14 operations substantially simultaneously.

1 40. A prime number generating system as recited in claim 39 wherein said processing
2 means is operative to develop said plurality of y additional odd numbers based on each
3 one of the randomly generated odd numbers $n_{0,0}, n_{1,0}, \dots, n_{(k-1),0}$ by successively adding
4 two to each of said randomly generated odd numbers $n_{0,0}, n_{1,0}, \dots, n_{(k-1),0}$ to provide $(k \times y)$
5 additional prime number candidates expressed as $(n_{0,1} = n_{0,0} + 2, n_{0,2} = n_{0,0} + 4, \dots, n_{0,y} =$
6 $n_{0,0} + (y \cdot 2)), (n_{1,1} = n_{1,0} + 2, n_{1,2} = n_{1,0} + 4, \dots, n_{1,y} = n_{1,0} + (y \cdot 2)), \dots, (n_{(k-1),1} = n_{(k-1),0} + 2, n_{(k-1),2} = n_{(k-1),0} + 4, \dots, n_{(k-1),y} = n_{(k-1),0} + (y \cdot 2))$.

1 41. A prime number generating system as recited in claim 39 wherein:

said processing means is operative to provide a plurality of t sets of test parameters associated with a plurality of t primality tests to be performed on each one of said plurality of $(k \times (y+1))$ randomly generated numbers, each of the $(k \times (y+1) \times t)$ sets of said test parameters including said associated one of said plurality of $(k \times (y+1))$ prime number candidates and an associated one of a plurality of t base values;

said plurality of exponentiation units includes a plurality of at least $(k \times (y+1) \times t)$ exponentiation units each being responsive to an associated one of said $(k \times (y+1) \times t)$ sets of said test parameters, and being operative to perform an exponentiation operation based on said associated set of test parameters, and also operative to generate a primality test result signal declaring said associated prime number candidate to be either composite or prime with reference to said associated base value, said plurality of at least $(k \times (y+1) \times t)$ exponentiation units being operative to perform said plurality of $(k \times (y+1) \times t)$ exponentiation operations substantially simultaneously.

42. A prime number generating system as recited in claim 36 wherein each of said primality tests is a Fermat type primality test.

43. A prime number generating system as recited in claim 36 wherein each of said primality tests is a Miller-Rabin type primality test.

44. A prime number generating system as recited in claim 36 wherein said processing means is operative to randomly generate said plurality of k random odd numbers by performing the steps of:

defining a length L for each of the plurality of k random numbers to be generated;
and
generating each of said plurality of k random odd numbers in an interval between 2^L and 2^{L-1} .

45. A prime number generating system for searching in parallel for a plurality of prime number values simultaneously, comprising:

processing means operative to randomly generate at least one random odd number providing a prime number candidate, and to determine a plurality of y additional odd numbers based on each of said at least one randomly generated odd number to provide y additional prime number candidates, thereby providing a total number of $y+1$ candidates, said processing means also being operative to provide at least one set of test parameters associated with a primality test to be performed on each one of said prime number candidates, each said set of test parameters including said associated prime number candidate and an associated base value; and

a plurality of exponentiation units each being communicatively coupled with said processing means, and being responsive to an associated one of said sets of test parameters, and operative to perform an exponentiation operation based on said associated set of test parameters, and also operative to generate a primality test result signal declaring said associated prime number candidate to be either composite or prime with reference to said associated base value, said exponentiation units being operative to perform said exponentiation operations substantially simultaneously;

said processing means being responsive to said primality test result signals, and operative to process said test result signals for the purpose of eliminating randomly generated numbers declared to be composite in accordance with a search for prime number values.

46. A prime number generating system as recited in claim 45 wherein said at least one randomly generated odd number is expressed as $n_{0,0}$, and wherein said processing means operative to determine said plurality of y additional odd numbers based on said randomly generated odd number by successively adding two to said randomly generated odd number $n_{0,0}$ to provide $(y+1)$ additional prime number candidates expressed as $(n_{0,1} = n_{0,0} + 2, n_{0,2} = n_{0,0} + 4, \dots, n_{0,y} = n_{0,0} + (y \cdot 2))$.

47. A prime number generating system as recited in claim 45 wherein:
said processing means is operative to provide a plurality of t sets of test parameters associated with a plurality of t primality tests to be performed on each one of said plurality of at least $y+1$ randomly generated numbers, each of the $((y+1) \times t)$ sets of

5 said test parameters including said associated one of said plurality of candidates and an
6 associated one of a plurality of t base values;
7 said plurality of exponentiation units includes a plurality of at least $((y+1) \times t)$
8 exponentiation units each being responsive to an associated one of said $((y+1) \times t)$ sets of
9 said test parameters, and being operative to perform an exponentiation operation based on
10 said associated set of test parameters, and also operative to generate a primality test result
11 signal declaring said associated prime number candidate to be either composite or prime
12 with reference to said associated base value, said plurality of at least $((y+1) \times t)$
13 exponentiation units being operative to perform said plurality of $((y+1) \times t)$
14 exponentiation operations substantially simultaneously.

1 48. A prime number generating system as recited in claim 45 wherein said processing
2 means is further operative to sieve said prime number candidates by performing a small
3 divisor test on each of said prime number candidates in order to eliminate candidates
4 revealed to be composite numbers by said small divisor test thereby yielding a sieved
5 number s of candidates.

1 49. A prime number generating system as recited in claim 45 wherein:
2 said processing means is operative to generate a plurality of k random odd
3 numbers each providing a prime number candidate, and to determine a plurality of y
4 additional odd numbers based on each of said k random odd numbers to provide $k \times y$
5 additional prime number candidates, thereby providing a total number of at least $k \times$
6 $(y+1)$ candidates, said processing means also being operative to provide at least one set of
7 test parameters associated with a primality test to be performed on each one of said $k \times$
8 $(y+1)$ prime number candidates, each said set of said test parameters including said
9 associated prime number candidate and an associated base value; and
10 said plurality of exponentiation units includes a plurality of at least $k \times (y+1)$
11 exponentiation units each being responsive to an associated one of said $k \times (y+1)$ sets of
12 said test parameters, and being operative to perform an exponentiation operation based on
13 said associated set of test parameters, and also operative to generate a primality test result
14 signal declaring said associated prime number candidate to be either composite or prime

15 with reference to said associated base value, said plurality of at least $k \times (y+1)$
16 exponentiation units being operative to perform said plurality of $k \times (y+1)$ exponentiation
17 operations substantially simultaneously.

1 50. A prime number generating system as recited in claim 45 wherein each of said primality
2 tests is a Fermat type primality test.

1 51. A prime number generating system as recited in claim 45 wherein each of said primality
2 tests is a Miller-Rabin type primality test.

1 52. A prime number generating system as recited in claim 45 wherein said processing means
2 is operative to randomly generate said plurality of k random odd numbers by performing the
3 steps of:

4 defining a length L for each of the plurality of k random numbers to be generated;

5 and

6 generating each of said plurality of k random odd numbers in an interval between
7 2^L and 2^{L-1} .

1 53. A prime number generating system for searching in parallel for a plurality of
2 prime number values simultaneously, comprising:

3 processing means operative to randomly generate a plurality of random odd
4 numbers each providing a prime number candidate, and to provide a set of test
5 parameters associated with a primality test to be performed on each one of said plurality
6 of randomly generated numbers, each said set of said test parameters including said
7 associated randomly generated number; and

8 a plurality of exponentiation units each being communicatively coupled with said
9 processing means, and being responsive to an associated one of said sets of test
10 parameters, and operative to perform an exponentiation operation based on said
11 associated set of test parameters and an associated base value, and also operative to
12 generate a primality test result signal declaring said associated prime number candidate to
13 be either composite or prime with reference to said associated base value, said

14 exponentiation units being operative to perform said exponentiation operations
15 substantially simultaneously;
16 said processing means being responsive to said primality test result signals, and
17 operative to process said test result signals for the purpose of eliminating randomly
18 generated numbers declared to be composite in accordance with a search for prime
19 number values.

1 54. A computer readable storage medium having stored thereon encoding instructions for
2 executing a process of searching in parallel for a plurality of prime number values
3 simultaneously in a prime number generation system including a processing unit and a plurality
4 of exponentiation units communicatively coupled with the processing unit, the process
5 comprising the steps of:

6 randomly generating a plurality of k random odd numbers each providing a prime
7 number candidate; and

8 performing at least one primality test on each of said candidates, each of said primality
9 tests including an associated exponentiation operation executed by an associated one of the
10 exponentiation units, said exponentiation operations being performed by said associated
11 exponentiation units substantially simultaneously.

1 55. A computer readable storage medium as recited in claim 54 wherein said plurality of k
2 randomly generated numbers are expressed as $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$, further comprising the steps
3 of:

4 determining a plurality of y additional odd numbers based on each one of the randomly
5 generated numbers $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$ to provide $(k \times y)$ additional prime number candidates $(n_{0,1}$
6 $, n_{0,2}, \dots n_{0,y}), (n_{1,1}, n_{1,2}, \dots n_{1,y}), \dots (n_{(k-1),1}, n_{(k-1),2}, \dots n_{(k-1),y})$ thereby yielding a total number of $(k$
7 $\times (y+1))$ prime number candidates;

8 wherein said step of performing includes performing a primality test on each of said total
9 number $(k \times (y+1))$ of candidates, each of the plurality of $(k \times (y+1))$ primality tests including an
10 associated exponentiation operation executed by an associated one of a plurality of $(k \times (y+1))$ of
11 the exponentiation units, said exponentiation operations being performed by said plurality of $(k \times$
12 $(y+1))$ exponentiation units substantially simultaneously.

1 56. A computer readable storage medium as recited in claim 55 wherein said step of
2 determining a plurality of y additional odd numbers based on each one of the randomly
3 generated numbers $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$ includes successively adding two to each of said randomly
4 generated odd numbers $n_{0,0}, n_{1,0}, \dots n_{(k-1),0}$ to provide $(k \times y)$ additional prime number candidates
5 expressed as $(n_{0,1} = n_{0,0} + 2, n_{0,2} = n_{0,0} + 4, \dots n_{0,y} = n_{0,0} + (y \cdot 2)), (n_{1,1} = n_{1,0} + 2, n_{1,2} = n_{1,0} + 4, \dots$
6 $n_{1,y} = n_{1,0} + (y \cdot 2)), \dots (n_{(k-1),1} = n_{(k-1),0} + 2, n_{(k-1),2} = n_{(k-1),0} + 4, \dots n_{(k-1),y} = n_{(k-1),0} + (y \cdot 2))$.

1 57. A computer readable storage medium as recited in claim 54 wherein said step of
2 performing includes performing a plurality of t primality tests on each one of said plurality of k
3 randomly generated numbers, each of the plurality of $(k \times t)$ primality tests including an
4 associated exponentiation operation executed by an associated one of a plurality of $(k \times t)$ of the
5 exponentiation units, said exponentiation operations being performed by said associated
6 exponentiation units substantially simultaneously.

1 58. A computer readable storage medium as recited in claim 55 wherein said step of
2 performing includes performing a plurality of t primality tests on each of said $(k \times (y+1))$ prime
3 number candidates, each of the plurality of $(k \times (y+1) \times t)$ primality tests including an associated
4 exponentiation operation executed by an associated one of a plurality of $(k \times (y+1) \times t)$ of the
5 exponentiation units, said exponentiation operations being performed by said plurality of $(k \times$
6 $(y+1) \times t)$ exponentiation units substantially simultaneously.

1 59. A computer readable storage medium as recited in claim 54 further comprising the steps
2 of:

3 sieving said prime number candidates by performing a small divisor test on each
4 of said candidates in order to eliminate candidates revealed to be composite numbers by
5 said small divisor test thereby yielding a sieved number s of candidates;

6 wherein said step of performing includes performing at least one primality test on each of
7 said sieved number s of candidates, each of the plurality of s primality tests including an
8 associated exponentiation operation executed by an associated one of a plurality of s of the
9 exponentiation units, said exponentiation operations being performed by said plurality of s
10 exponentiation units substantially simultaneously.

1 60. A computer readable storage medium as recited in claim 55 further comprising the steps
2 of:

3 sieving said prime number candidates by performing a small divisor test on each
4 of said number $(k \times (y+1))$ of prime number candidates in order to eliminate candidates
5 revealed to be composite numbers by said small divisor test thereby yielding a sieved
6 number s of candidates;

7 wherein said step of performing includes performing at least one primality test on
8 each of said sieved number s of candidates, each of the plurality of s primality tests
9 including an associated exponentiation operation executed by an associated one of a
10 plurality of s of the exponentiation units, said exponentiation operations being performed
11 by said plurality of s exponentiation units substantially simultaneously.

1 61. A computer readable storage medium as recited in claim 54 further comprising the step
2 of:

3 sieving said prime number candidates by performing a small divisor test on each
4 of said candidates in order to eliminate candidates revealed to be composite numbers by
5 said small divisor test thereby yielding a sieved number s of candidates;

6 wherein said step of performing includes performing an associated first one of t primality
7 test on each of said sieved number s of candidates, each of the plurality of s first primality tests
8 including an associated exponentiation operation executed by an associated one of a plurality of s
9 of the exponentiation units, said first exponentiation operations being performed by said plurality
10 of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to
11 be composite numbers by said first primality tests thereby yielding a remaining number r of
12 candidates; and

13 performing a plurality of $t-1$ additional primality tests on each of said remaining number
14 r of candidates, each of the plurality of $(r \times (t-1))$ primality tests including an associated
15 exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the
16 exponentiation units, said $(r \times (t-1))$ exponentiation operations being performed by said plurality
17 of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further
18 candidates revealed to be composite numbers.

1 62. A computer readable storage medium as recited in claim 55 further comprising the steps
2 of:

3 sieving said prime number candidates by performing a small divisor test on each
4 of said number $(k \times (y+1))$ of prime number candidates in order to eliminate candidates
5 revealed to be composite numbers by said small divisor test thereby yielding a sieved
6 number s of candidates;

7 wherein said step of performing includes performing an associated first one of t primality
8 tests on each of said sieved number s of candidates, each of the plurality of s first primality tests
9 including an associated exponentiation operation executed by an associated one of a plurality of s
10 of the exponentiation units, said first exponentiation operations being performed by said plurality
11 of s exponentiation units substantially simultaneously in order to eliminate candidates revealed to
12 be composite numbers by said first primality tests thereby yielding a remaining number r of
13 candidates; and

14 performing a plurality of $t-1$ additional primality tests on each of said remaining number
15 r of candidates, each of the plurality of $(r \times (t-1))$ primality tests including an associated
16 exponentiation operation executed by an associated one of a plurality of $(r \times (t-1))$ of the
17 exponentiation units, said $(r \times (t-1))$ exponentiation operations being performed by said plurality
18 of $(r \times (t-1))$ exponentiation units substantially simultaneously in order to eliminate further
19 candidates revealed to be composite numbers.

1 63. A computer readable storage medium as recited in claim 59 further comprising the steps
2 of:

3 receiving a specified public exponent e associated with a cryptographic application;
4 testing the suitability of each of said prime number candidates for use in said
5 cryptographic application by testing the relative primality of each said prime number candidate
6 minus one and said specified public exponent e , wherein said step of testing the suitability is
7 performed prior to said step of performing at least one primality test.